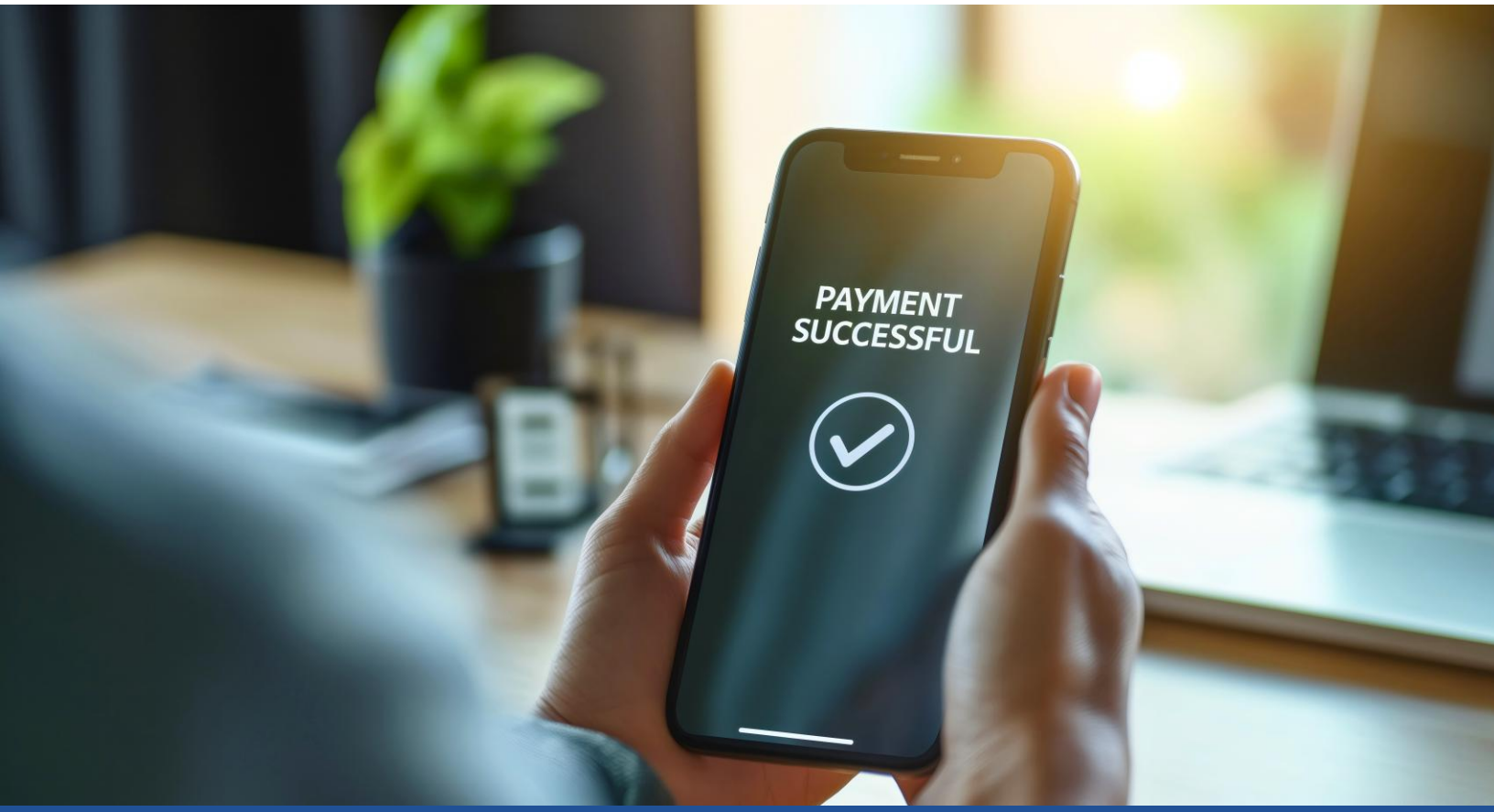


Guideline.02: Operational Considerations for Instant Payments Send-Side Primer

Fasterpaymentscouncil.org

January 2025

Table of Contents

This document provides best practices and considerations for financial institutions. The content is not intended to be exhaustive, and each institution should consult with its own legal, compliance, and other relevant professionals regarding implementation. The information presented is current as of the publication date.

The Clearing House Payments company did not write this document and is not responsible for any inaccuracies about the RTP® Network, the laws and regulations relevant to instant payments, or payment systems generally.

Introduction

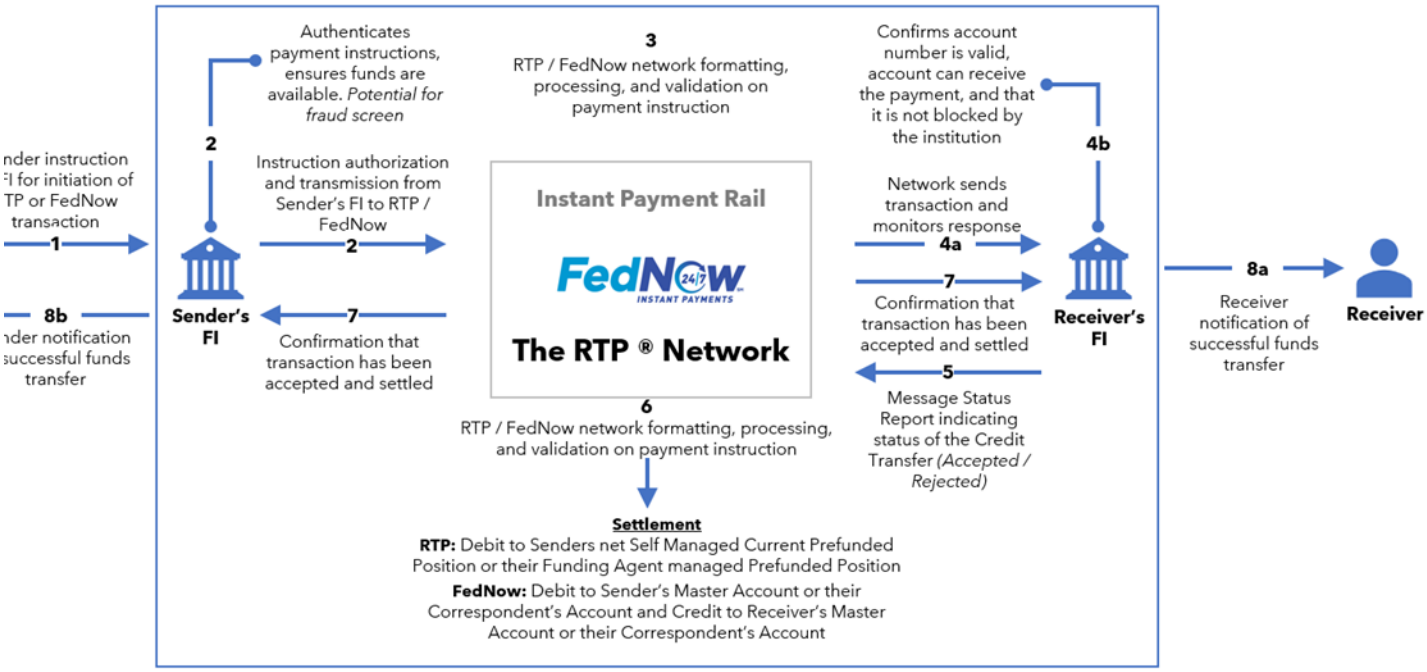
A financial institution's strategic roadmap for instant payments adoption should not end with receive-side capabilities. Financial institutions (FIs) can benefit from advances in U.S. instant payment offerings, particularly by participating in sending instant payments.

The Faster Payments Council's (FPC) Operational Considerations for Instant and Immediate Payments Work Group continues to identify and report guidelines for FIs adopting instant payments. This document serves as a primer on send-side operational considerations for implementing instant payments, offering high-level insights on priorities to consider when expanding capabilities beyond receiving. For more information on receiving instant payments, see the Operational Considerations for Receiving Instant Payments Guideline.[1] These primers provide valuable foundational information on instant payments, including specific considerations, and can be used as resources to increase knowledge of instant payments.

This document introduces the following operational components, each of which will be explored in greater detail in subsequent guidelines:

1) Instant Payment Send Flow
2) Interoperability & Routing Considerations
3) User Experience and User Interface – Financial Institution Application / Portal for Instant Payments
4) Liquidity Management
5) Real-Time Reconciliation for Outgoing Funds
6) Business Continuity & Resilience
7) Staffing Needs & Training Requirements
8) Accountholder Support, Education & Disclosures
9) Fraud Mitigation
10) Compliance
11) Exception Processing
12) Mechanisms for Achieving Performance Requirements

1) Instant Payment Send Flow



Traditional payment flows have historically been single-directional. The sending FI initiates the payment and assumes success unless it is returned. This lack of immediate feedback meant the only way to determine the outcome was either a returned payment or no response at all, indicating successful receipt. In contrast, instant payments (as detailed in the diagram above) are conversational. The payment enters the network, and an immediate response confirms success or failure, assuring the sender of receipt. This confirmation means the receiving FI has received the payment and the funds are available to the recipient.

Traditional payment rails do not have message capabilities that support error resolution between senders and receivers. While Fedwire® Funds Service and CHIPS® support limited messaging functionality, the responses are not mandated as they are with both the FedNow® Service and the RTP® network. FedNow and RTP network allow senders to request information or request a return of funds, with receivers able to respond through the network. However, despite this communication channel, both FedNow and RTP payments are irrevocable, meaning the receiving FI is not obligated to return the payment. The detailed guidelines will expand upon these flows and offer suggestions on how FIs can leverage them to create a new payment experience for their account holders.

2) Interoperability & Routing Considerations

Interoperability Models

Integration at the network level is not available for FedNow Service and RTP Network at the time of this primer's publishing. In contrast to the full interoperability of the ACH Network between network operators, where an ACH transaction sent through one operator can be received through the other. One way to achieve interoperability is through a routing model between instant payment networks, which involves connection to the end points of both networks. With this model, FIs could send and receive payments on both networks based on predefined routing logic. Third-party service providers (TPSPs) ease the burden of interoperability concerns by facilitating routing and standardizing payment messages to process and settle transactions with either instant payment network.

Routing Rule Drivers

1. **Financial Institution Availability:** Both the sending and receiving FIs in a FedNow or RTP transaction need to be enabled participants on the respective network. To ensure higher success rates on instant payment requests, FIs can leverage resources at both the Federal Reserve and TCH to identify receive-capable FIs and their enabled participation types.[2] The FedNow interface offers a participant list that reflects whether a participating FI is enabled for receive customer credit transfers, send, and receive credit transfers, or receive requests for payment. The RTP and FedNow networks both provide a nightly file as well that identifies Routing Transit Numbers (RTNs) for participating FIs.[3] There are TPSPs offering a single endpoint to access directories for RTP and FedNow participation status lookup.

2. **Network Fees:** Financial institutions should analyze fee structures for both FedNow and RTP on a per-transaction basis, volume-based pricing, and other fees, including overhead.[4]

3. **Dollar Limitations at Network Level:** Dollar limits per transaction must be a consideration for routing large payments, as the limit for FedNow is $500,000 and that of RTP is $10,000,000.[5]

4. **Financial Institution Preference:** Financial institutions may base their routing rules upon their relationships with network operators, their technical capability, or their business strategy.

Contingency Planning – Alternative Payment Methods

When FedNow and RTP are unavailable for a specific payment, financial institutions may consider the ACH network or Wire transfers as a fallback alternative payment method. ACH offers a reliable alternative for instant payment rails given characteristics including its widespread adoption amongst U.S. FIs, minimal dollar limitations at the network level, and low fees. However, ACH's deferred net settlement and less time-sensitive nature—amongst other characteristics, rules, regulations, and formats—may also render ACH untenable for the specific payment use case. As such, ACH may not always be a viable fallback option for RTP and/or FedNow. Wire transfers may alternatively offer benefits including fast settlement of funds; however, wires are often more costly than alternatives and are not available 24x7x365, amidst other considerations. Decisions regarding fallback options should align with the best needs of the product or use case itself.

3) User Experience and User Interface – Instant Payments Application / Portal

Financial institutions should approach User Experience (UX) and User Interface (UI) design from two distinct but equally important perspectives: the customer's experience and the FI staff members' experience. The customer's experience involves how an end user initiates a payment, views the results, etc. FI staff members manage real-time payment activities, handling exceptions, and performing reconciliation tasks, among other responsibilities.

While UX/UI exists for many other types of payments, a key difference with real-time payments is the speed and finality of these transactions. From the customer's standpoint, the UX/UI must prioritize simplicity, speed, and security. The interface should be intuitive, minimizing the steps required to complete transactions. Key features should include intuitive navigation, clear instructions, and instant feedback on transaction status. Security measures, like multi-factor authentication, should be seamlessly integrated to protect users while minimizing friction.

Given the additional data that can be present in an ISO 20022 message, which both RTP and FedNow utilize, it is critical to evaluate whether existing platforms, such as mobile apps or web applications, are designed with the necessary fields and can deliver the swift responses that instant payments require. If the institution handles both RTP and FedNow services, it should consider a unified interface that can distinguish between them or aggregate them under a general "Instant Payments" category. Implementing preventive measures, like a verification "speedbump" to confirm details before finalizing transactions, enhances safety and reduces the risk of mistakes and fraud by ensuring that users double-check crucial information. However, at the same time, this may introduce friction into the user experience, so a UX/UI evaluation must determine where that friction makes sense and where it does not.

Conversely, the interface for staff should bolster effective management and oversight of payment operations. As with the customer experience, the key difference for real-time payments is the finality and speed of these transactions, necessitating different UI features for bank staff. It needs to deliver clear, instant visualizations of data and provide tools for rapid response to issues. The system should facilitate a streamlined workflow that supports managing large transaction volumes efficiently and accurately. Additionally, the system should allow financial institutions to configure transaction limits based on their defined risk appetite.

Real-time updates on payment status (e.g., moving beyond end-of-day reports) can significantly improve reconciliation efforts. Because instant payments are irreversible, it is essential to have robust systems for handling exceptions or return requests.

Again, if the institution handles both RTP and FedNow services, it should consider a harmonized interface that can distinguish between them or aggregate them under a general "Instant Payments" category. Consistency in payment entry fields across all platforms is crucial to avoid confusion and enhance usability. Seamless integration with third-party services and compliance with ISO messaging standards are essential for ensuring efficient transaction processing and system interoperability.

By effectively addressing these considerations, financial institutions can deliver a seamless, secure, and efficient payment experience that meets the needs of both customers and staff.

4) Liquidity Management

Liquidity management is crucial for participating in instant payment networks. Introducing send functionality requires additional due diligence and risk management. Financial institutions must navigate prefunding requirements for the RTP network, manage liquidity risks, and utilize specific tools to ensure seamless transaction processing and compliance with regulatory standards. Below are key considerations or tools FIs should familiarize themselves with prior to implementing send functionality.

Prefunding Considerations: When participating in the RTP Network, FIs are required to prefund their RTP Account via the joint account to facilitate real-time settlement of transactions. FedNow does not require prefunding as FIs are able to utilize their existing Master Account or a correspondent account. The Clearing House determines prefunding requirements based on tiers structured around U.S. transaction deposit ranges for each FI. This prefunding ensures that funds are immediately available for settlement when transactions occur. Transactions will process as long as funds are in the joint account, however, if the account goes below zero, the transaction(s) will be rejected.

Watermarks: The RTP network offers watermark functions which are intended to help FIs manage their liquidity and funding requirements.

Funding RTP Account: Financial institutions can fund their RTP account via wire transfer through the joint account and can monitor their liquidity positions through the RTP Management Portal.

Management of Liquidity: Effective liquidity risk management is essential to handle unexpected spikes in payment volumes or amounts. FIs should incorporate instant payments in their forecasting models to mitigate risk and ensure continuous service availability. Understanding projected transaction volumes from both sending and receiving perspectives is crucial for accurate liquidity forecasting, including overnight and weekend transactions.

FedNow: FedNow utilizes an FI master or correspondent account, allowing FIs to leverage their existing tools for liquidity management. Unlike the RTP Network, FedNow transactions will technically continue to process (even if the master account does not have sufficient funds to cover the transaction(s) (although Fed Guidance is that the accounts should not be utilized in this way), which makes it imperative for FIs to actively monitor and manage liquidity in order to avoid any potential overdrafts and violation of network rules.

Liquidity Management Transfer: To support instant payment liquidity needs, the liquidity management transfer (LMT) is available and enables FedNow Participants to send funds to each other. LMTs are available from 7 pm to 7am ET on weekdays, and 24 hours per day on weekends and holidays.

Funding Agents/Correspondent Accounts for Enhanced Liquidity Management: For FIs who prefer not to manage liquidity directly, funding agents such as Bankers Banks and Corporate Credit Unions, or utilizing correspondent banks may be good options. These entities offer payments and liquidity funding services, assisting FIs in meeting their liquidity obligations efficiently.

Effective liquidity management is crucial for FIs participating in instant payment systems. By managing transactional liquidity, utilizing advanced forecasting, and leveraging liquidity management tools like watermarks and funding agents, FIs can ensure compliance, mitigate risk, and provide reliable instant payment services to their customers.

5) Real-Time Reconciliation for Outgoing Funds

Effective reconciliation of outbound Real-Time Payments (RTP) hinges on real-time data management and robust automation. The FI must ensure their systems can process transactions instantaneously, maintaining up-to-date ledgers and transaction records. Integrating these systems with Enterprise Resource Planning (ERP) solutions is essential for synchronized data flow, providing real-time visibility across departments and minimizing errors through automation.

Adhering to regulatory requirements and generating comprehensive reports ensure transparency and accountability. Exception handling processes must be in place to quickly identify and resolve discrepancies, supported by automated alerts and workflows.

Scalability and interoperability further enhance the reconciliation process. Systems must be designed to handle increasing transaction volumes without compromising performance, ensuring they can scale with business growth and facilitate seamless interactions across the financial ecosystem. This compatibility with various payment networks and platforms facilitates reconciliation efficiency and accuracy.

Financial institutions can leverage their existing reconciliation processes for receiving instant payments to accommodate the origination side. It is important to consider real-time message reconciliation, end-of-day reconciliation, and reconciliation with accountholders and internal general ledger accounts.

6) Business Continuity & Resilience

Due to their real-time nature, instant payments carry inherent risks and challenges that should be considered for business continuity and resilience planning.

- There is typically a financial driver behind the need to send funds in real-time, so if a transaction fails, there is a risk of financial hardship and/or reputational damage for the customer and the organization (ex. fines for late payment, services shut down for late payment, eviction, an asset not secured due to untimely payment, etc.).

To mitigate these risks, financial institutions should ensure adequate staffing with trained personnel who are familiar with instant payment operations. Understanding the escalation procedures and service level agreements (SLA) of vendor partners is crucial to maintain operational continuity in case of system disruptions. Additionally, FIs should understand which vendors are critical to instant payment processing performance and ensure they have thorough back up or failover plans.

Business continuity plans should be updated to include instant payments, incorporating considerations like liquidity management and reconciliation processes. It is important to have monitoring systems to be able to detect when there are system interruptions or transaction discrepancies on the sending and receiving of payments. If required, an authorized user should have the capability to override the system to bypass failure points caused due to technical issues or limitations. Additionally, the financial institution should have a process to shut down the instant payment transaction processing if/when necessary (e.g., fraud attacks). Another important consideration is the ability to access and address low-liquidity scenarios to ensure continuous operations.

7) Staffing Needs & Training Requirements

Enabling sending instant payments introduces a new dynamic to an institutions' staffing and training needs. While the core functions and capabilities such as the real-time and irrevocable nature should remain part of ongoing training and education, considerations for customer- facing staff supporting instant payment use cases, it is important to consider the following:

1. Front Office vs. Back Office: The policies, systems, tools, and resources that enable effective job performance, in turn contribute to seamless customer experience, and proactively manage and mitigate risks for the financial institution. This should include consideration of functional areas and stakeholders across the institution. More specific topics that will be detailed in the subsequent guidelines include the need for front line and operations staff to be trained in how to handle an unauthorized instant payment, requests for returns, managing and leveraging network negative lists, and other topics. Customer-facing and operations areas will need to work with compliance and determine documents that may be needed to support customer requests such as for unauthorized transactions or changing limits.

2. Sales and Product Support: Effective approaches for sales, pricing, onboarding, and support for accountholders originating instant payments should all be considered. These roles also contribute to ongoing risk management through activities such as setting limits and understanding risk across all products.

3. Other Staffing: Staffing needs will be driven by specific use cases and the accessibility of the systems that are utilized for payment origination, as well as payment volume. A use case with higher volume, complex systems or processes, and systems available 24x7x365 may warrant additional staffing in areas like call centers, fraud prevention, information technology, and product support. Specific consideration should be given to support nights, weekends, and holidays if the service is available to end users during those times.

It will also be important to reassess needs as demand for instant payments increases, use cases expand, and volume grows within the financial institution.

8) Accountholder Education & Disclosures

Education

An effective way to highlight the benefits of Instant Payments for an FI's accountholders is to develop brief use cases that are unique to a financial institution. Options include use cases for Me to Me, Small Businesses, or Me to You. Once use cases are defined, FIs can show their accountholders how easy the process is with screen shots. Customer–facing employees should visualize how the product will work and determine the questions that the end user may ask. Some core questions to address could be: *Where is my payment? How do I increase/decrease my limit? What if I do not recognize this payment?* Once the list of questions is developed, it can be populated with responses and then provided to the financial institution's marketing team.

In addition to use case specific education, corporates and consumers should also be educated on how instant payments work at a high level. This should include key features of instant payments like irrevocability, how fast payments process, how requests for return of funds work, and what information or notifications the sender may receive associated with a transaction. Any restrictions or limitations of the product or use case should also be clearly communicated and disclosed. This may include limitations on the hours or days sending is available, restrictions related to funds availability, and what happens if there is an error or other exception with the payment. There should also be continual education on scams as they are constantly changing.

Disclosures of products or origination services

An attorney should review the FIs disclosures and any agreements regarding instant payments. For both businesses and consumers, disclosures should address transaction limits, timing for receipt of funds, funds availability, the exceptions and investigation process, payer authorization, handling disputed payments, and fees. For consumers, additional disclosures may be required, including per the EFTA and Regulation E as well as privacy laws.

9) Fraud Mitigation

The implementation of send capabilities introduces fraud risks that are different than those which exist when receiving instant payments, but are not dissimilar to fraud risks present in other traditional payment channels, such as ACH, wire transfer, check, etc. As a result, many of the internal controls that are effective in fighting fraud in traditional payment systems are also beneficial when applied to mitigating fraud related to sending instant payments.

First, it is recommended to establish fraud controls that are commensurate with the financial institution's unique instant payments risk environment, particularly regarding transaction volume and user type. High-volume transactions, especially in commercial settings, necessitate stricter controls and real-time monitoring due to increased fraud exposure. Conversely, consumer transactions, typically lower in value and frequency, may have different control measures and frequencies. By assessing risk profiles and adjusting controls accordingly, financial institutions can effectively balance security and efficiency, ensuring that instant payments are both safe and seamless for all users.

Below are some examples of fraud controls to consider in a faster payment fraud mitigation program for financial institutions with send capabilities.

1. **Digital Profiling:** Digital profiling leverages data such as device fingerprints, IP addresses, and behavioral patterns to identify legitimate users. Digital profiling should be configured to accurately distinguish common behaviors of a legitimate user sending instant payments from unusual send activity from a user whose activity is outside of the realm of the consumer's typical behavior and/or location, which could indicate an account has been compromised.

2. **Real-Time Fraud Screening:** Real-time fraud detection systems identify patterns and outliers, flagging suspicious activities for further review. For instance, sudden high-value transactions or a spike in transaction frequency can trigger alerts, prompting immediate action to prevent fraud. Without real-time fraud screening, funds can be transferred out of an account within seconds, without the guarantee of recovering any of the losses.

3. **Category and Transaction Limits:** Category limits restrict transactions by type, while daily and weekly aggregated limits cap the total transaction value within specified periods. These controls help mitigate risks, particularly for high-value transactions or those prone to fraud. For example, establishing a daily limit on the number of transactions an individual can send as a faster payment transaction may prevent an unauthorized user from the ability to completely drain an account in a matter of seconds.

4. **Payee Validation:** As credit push payments, confidence that a sender is sending funds to the intended party and for legitimate reasons is of paramount importance. To meet this need, two types of payee confirmation are beneficial: a) verification that the sender knows the recipient and that funds are not being sent for fraudulent reasons, and b) verification of account name and number match. Payee validation is not currently embedded into the faster payment networks and would likely require a supporting service to be created and utilized.

5. **Account Validation**: Like payee confirmation, account validation processes verify the legitimacy of the account details before transactions are processed, adding another layer of security. Account validation is baked into faster payment systems since a transaction sent to a participating financial institution should be rejected if the account number is not valid.

6. **Multifactor Authentication:** Multifactor Authentication (MFA) adds a critical layer of security, requiring users to provide two or more verification factors. This could include something they know (password), something they have (smartphone), or something they are (fingerprint). As it relates to sending instant payments, the ability to prevent unauthorized access to a customer's online or mobile account using MFA can prevent the ability for fraud to be executed.

7. **Artificial Intelligence:** AI systems analyze vast amounts of data quickly, identifying suspicious patterns that human analysts might miss.

As noted above, many of the controls needed for instant payments are like those already used for existing payment systems, with minor variations. As fraud continues to evolve on all payment rails, financial institutions and other participants in the instant payments systems will need to remain vigilant in their efforts to combat fraud. For more information of fraud trends in faster payments, see the FPC's publication on "Faster Payments Fraud Trends and Mitigation Opportunities" (FPC, 2024).[6]

10) Compliance Programs that Encompass KYC/KYB and AML Obligations

Financial institutions and their service providers must navigate a complex web of risks and regulations when sending instant payments. Key areas to address include:

1. **Board-Approved Risk Mitigation Policy:** Establish a board-approved policy outlining risk mitigation strategies for instant payments. This includes impacts on roles, customer-facing systems (statements, online banking, dispute resolution), internal controls, monitoring, reporting, and training requirements.

2. **Compliance with Operating Rules:** Ensure compliance with the FedNow® Operating Circular 8 and The Clearing House's RTP requirements, including oversight of service providers. Ensure internal systems and those of any service providers can handle integration, including adapting to the ISO® 20022 messaging standard for interbank communication and having a plan for troubleshooting and ongoing monitoring.

3. **Service Provider Management:** A service provider's risk management framework for instant payment should align with the financial institution's risk appetite and clearly define roles and responsibilities for both parties. The agreement should address critical areas like data security, customer privacy, transaction processing, and incident response procedures.

4. **Customer Onboarding and KYC:** Evaluate KYC standards to determine if additional due diligence is needed for instant payment users.

5. **Transaction Monitoring:** Verify that transaction monitoring systems (fraud detection, sanctions screening, AML) can effectively manage the risks of instant funds movement.

6. **Disclosures and Authorizations**: Refine disclosures to clearly communicate risks, costs, funds availability, security, and potential outcomes of using instant payments. Obtain and retain appropriate user authorizations.

7. **Sending Timeframes and System Shutoff:** Determine if 24x7x365 sending is appropriate or if limitations are necessary. Implement system shutoff capabilities to manage risk in unforeseen circumstances.

The speed and irrevocable nature of instant payments for consumers necessitates a focus on fair and responsible practices. Financial institutions and their service providers should prioritize consumer protection principles outlined by the Consumer Financial Protection Bureau (CFPB) to ensure a safe and trustworthy experience, including equitable access, enhanced disclosures, data transparency and control, real-time communication, and authorization flexibility.

11) Exception Processing

When it comes to sending instant payments, it will largely depend on each financial institutions' preferences, risk appetite, and desired customer experience in terms of the degree and volume of exceptions they may utilize or experience. The use of systematic controls and automatic exception processing should be considered to streamline operations and customer experience. There are also differences in the type of exception that may be created including more back-office exceptions like fraud, AML, insufficient funds, or customers facing exceptions like failed or timed out payments, missing or inaccurate data, etc. All these circumstances should be evaluated to determine what parameters should trigger exceptions and how those exceptions will be handled.

Outside of product or use case specific exceptions, financial institutions should be prepared to support processing of outbound Request for Return of Funds (RFRF) whether the intake is through customer facing applications or manual based procedures. It will be important to build systems and processes to support timely and accurate processing, mechanisms for communicating status and results with the account holder, along with timely crediting of the customer's account when applicable.

12) Mechanisms for Achieving Performance Requirements

In the dynamic sector of instant payments, adhering to exacting performance standards is pivotal. From a business and user perspective, performance encompasses rapid transaction completion. Technically, it involves having the requisite infrastructure to efficiently meet these standards. The RTP network and FedNow put forward an SLA of being able to complete the end-to-end payment cycle within 15-20 seconds, which necessitates a high-performance system. The expectation is also to give customers the ability to initiate payments 24x7x365, which requires the systems to have high availability and reliability. This section of the document focuses on various considerations for supporting sending RTP and FedNow transactions.

High performance and availability of the systems:

For supporting 24x7x365 payments with SLA of 15-20 seconds, all systems involved in the payment system needs to be scaled to meet the demands. These are not limited to the systems directly involved with exchanging and processing payments messages but also other systems which are part of payment life cycle such as core banking systems, fraud, compliance checks, etc. Each of the systems should respond to requests promptly to be able to meet the overall SLA. The infrastructure can ideally be designed with stand-in processes along with end-of-day processing where applicable, so that the systems and services are available 24x7x365 without maintenance downtimes. These also include downtimes due to deployments of updates and patches.

Modernize / Upgrade architecture:

Higher performance output and stability can be achieved using modern cloud-based solutions and microservices architecture using APIs. Outsourcing managed services that simplify infrastructure management, along with suitable disaster recovery (DR) solutions and continuous and automated monitoring of the systems, is a key aspect to consider. The infrastructure should also be reviewed to reduce end-to-end network latency.

Upgrade and optimized workflow and designs:

Considering the high SLA for completion of payments and expected increase in future volume, optimizing the workflow and interface design would be a strategic need. With microservices architecture, the workflow should be optimized with rational service calls to avoid performance issues and race conditions. Similarly, the UI design can be reviewed to ensure a balance between UX and optimal performance of the system. This should factor in the various channels and platforms from where an instant payment can be initiated. As an example, initiation of payments using a mobile channel will have to factor in unstable mobile internet connectivity. The expected performance of the system should be driven by the use cases of the financial institution's client and not limiting the design to the higher end of the expected SLA by the payment network.

Straight Through Processing (STP):

Straight through processing of most payments is critical to maintain good user experience. The solution architecture, the process flows, and management of reference data should be done to reduce the dropout of payments into a manual queue. The rules configured for checks such as fraud and compliance should be adequate to meet compliance requirements but managed to reduce false positives.

Scalable solution:

It is essential that the infrastructure be designed for scaling to meet not just the current demands, but also the future expected and peak load demands. The cost to upgrade the infrastructure and ongoing cost for owning and maintaining the infrastructure would play a significant role in deciding if the solution would be hosted in the cloud or on-premises.

Conclusion

This primer provides a continued foundation for financial institutions to plan and refine their adoption of instant payments by providing high-level insights into key considerations. The different topics addressed are focal points that the team of experts on the FPC Operational Considerations for Instant & Immediate Payments Work Group felt were most important to consider. Subsequent guideline deliverables will cover greater detail regarding the sending side of instant payments as well as non-value messages (Request for Information, Request for Payment, Request for Refund).

Beyond the scope of the primer and subsequent guidelines, it is recommended that financial institutions also look at other areas to learn what they need for implementation of instant payments. While there are many operational and procedural challenges when implementing instant payments, there are lessons that can be learned within the institution's experience with retail point-of-sale, ATM usage, and card processing, as they work continuously in 24x7x365 environments. Additionally, lessons can be learned from other countries and institutions that have implemented instant payments.

Acknowledgements

Operational Considerations for Instant & Immediate Payments Work Group

Thank you to the members of the FPC Operational Considerations for Instant & Immediate Payments Work Group (OCWG), sponsored by Endava, who contributed to these guidelines.

OCWG Leadership

Miriam Sheril (Chair), Form3 US Inc.
Tony Cook (Vice Chair), FirstBank
Kevin Michels (FPC WG Facilitator), Guidehouse

OCWG Contributors

FPC Member Organization	Representative
Alloya Corporate FCU	Lisa Richmond
BHMI	Donna Blum
BOK Financial	Dana Woller
Cross River Bank	Sriram Iyer
EPCOR	Nicole Payne
FirstBank	Maranda Blake
JJ4Tech	Caroline Serejo Cypriano
Nacha	Mark Dixon
PaymentsFirst Inc. formerly Macha	Mary Gilmeister
PaymentsFirst Inc.	Jeanette Waye
RedCompass Labs	Stephen King
RedCompass Labs	Sudeep Manchanda
Reef Karson Consulting, LLC	Rodman Reef
Sphere Laboratories, LLC	Anthony Serio (Editor)
TransactionBanker.com	Barry Tooker
Wespay	Nathan Carman
Zumingo Inc.	Brian Libonate

About the U.S. Faster Payments Council and the Operational Considerations for Instant & Immediate Payments Work Group

The Faster Payments Council (FPC) is an industry-led membership organization whose vision is a world-class payment system where Americans can safely and securely pay anyone, anywhere, at any time and with near-immediate funds availability. To further this vision, the Faster Payments Council established the Operational Considerations for Instant & Immediate Payments Work Group to provide financial institutions with guideposts to effectively manage operational change that instant and immediate payments have on bank operations.

References

[1] Faster Payments Council. (2024, September). *Operational Considerations for Receiving Instant Payments.* https://fasterpaymentscouncil.org/userfiles/2080/files/OCWG_Operational%20Considerations%20for%20Receiving%20Instant%20Payments%20Guideline_09-12-2024%20Final.pdf.

[2] The Clearing House (n.d.). *RTP®: Routing/Transit Numbers.* Retrieved January 6, 2025, from https://www.theclearinghouse.org/payment-systems/rtp/rtn; The Federal Reserve Financial Services. (n.d.). *FedNow® Service Participants and Service Providers.* Retrieved January 6, 2025, from https://www.frbservices.org/financial-services/fednow/organizations.

[3] The Federal Reserve Financial Services. (2024, September 7). *The FedNow® Service Readiness Guide.* https://explore.fednow.org/resources/customer-readiness-guide.pdf.

[4] The Clearing House (n.d.). *RTP®: Real-Time Payments for All Financial Institutions.* Retrieved January 6, 2025, from https://www.theclearinghouse.org/payment-systems/rtp; The Federal Reserve Financial Services. (n.d.). *FedNow® Service 2024 Fee Schedule.* Retrieved January 6, 2025, from https://www.frbservices.org/resources/fees/fednow-2024.

[5] The Clearing House (2024, December 4). Higher $10 Million RTP® Network Transaction Limit Empowers New Uses. https://www.theclearinghouse.org/payment-systems/Articles/2024/12/Higher_10_Million_RTP_Network_Transaction_Limit_Empowers_New_Uses_12-04-2024.

[6] Faster Payments Council. (2024, January). *Faster Payments Fraud Trends and Mitigation Opportunities.* https://fasterpaymentscouncil.org/userfiles/2080/files/FPC%20Fraud%20Bulletin_01_01-24-2024_Final.pdf.